

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:	William J. Eakin	Examiner:	Stephen D'Agosta
Serial No.:	10/685,366	Group Art Unit:	2617
Filed:	October 14, 2003	Docket No.:	10018596-1
Title:	System and Method for Remotely Accessing a Private Database		

REPLY BRIEF UNDER 37 C.F.R. § 41.41

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

In response to the Examiner's Answer mailed 01/05/2007, Appellants file this Reply Brief in accordance with 37 C.F.R. § 41.41.

AUTHORIZATION TO DEBIT ACCOUNT

It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's deposit account no. 08-2025.

Status of Claims

Applicants acknowledge that the status of the claims is as follows:

Claims 7-9, 10-11, and 18 are objected to but would be allowed if rewritten in independent form to include all limitations of the base claim and any intervening claims.

Response to Examiner's Arguments

Appellants focus the Reply Brief on the following issue: Does the art of record teach or suggest each element in the claims? The art of record does not. Some examples are provided below.

By way of example, independent claims 1, 12, 19, 22, 24, 25, and 27 recite that “verification of only the appliance ID is sufficient to authorize access to the private database” (emphasis added). Applicants respectfully ask the Board of Appeals to give weight to each and every word in the claim. The art of record does not disclose or even suggest verifying “only” the appliance ID to authorize access to a private database.

The Examiner provides several different arguments stating that the combination of Garrison and Rezvani teach or suggest this element. Appellants respectfully disagree and address these arguments.

First, in section V of the Answer brief, the Examiner argues:

The prior art cited provides considerable more security than the appellant and thus would have used only an appliance ID many “generations” ago, meaning authentication processes have evolved from “verifying though an in-person visit” (eg. when using a notary) to remotely authenticating a user (eg. such as taught by Garrison). (See Examiner’s Answer at p. 20).

Appellants strongly disagree because the statements of the Examiner are not supported in the art. The Examiner states his own personal beliefs and conclusions without support from the actual teachings in the references themselves. Where does the

combination of Garrison and Rezvani teach or suggest that appliances developed “generations” ago used only an appliance identification to authorize access to a private database? Garrison and Rezvani do not state or suggest such teachings.

In contrast to providing personal beliefs, Appellants provide arguments based on teachings actually in the references. Fig. 4A in Garrison is a flowchart that describes the complex key exchange between a user and a server in order to identify a user and grant access to the server. Garrison states how the access is performed:

After receiving the new encryption key from the server 17a, the client 14 encrypts the user’s password and log name with the new encryption key and transmits the password and log name to the server 17a

The server 17a compares the log name transmitted by the client 14 with the log name in the password data table entry corresponding with the password. If the log names match, the user of the client 14 is determined to be an authorized user. (See [0066 – 0067]: portions omitted for brevity).

Garrison expressly states that a user must send a password and login name so the server can verify the user. Garrison repeatedly teaches that his access request identifies the user, not the wireless device. Nowhere does this section or any section of Garrison (alone or in combination with Rezvani) teach or suggest that verification of only the application ID is sufficient to authorize access to the private database.

Paragraph [0004] of Rezvani states that cellular phones have electronic subscriber numbers (ESNs) that uniquely identify the cellular phone. Paragraphs [0108-0111] of Rezvani state that various communication links can be used to connect a wireless device with a server. Finally, paragraph [0113] of Rezvani states that the wireless device can be various embodiments, such as cellular phones, personal digital assistants, and computers. Notice, however, that nowhere does Rezvani (alone or in combination with Garrison) teach or suggest whatsoever that the ESN itself is used to provide access to a private

database. In other words, Rezvani teaches that ESNs on cellular phones are known. But, Rezvani never teaches or suggests that only the ESN is sufficient to authorize access to a private database.

Second, in section VI of the Answer brief, the Examiner argues that Garrison inherently teaches the claim element of “verification of only the appliance ID is sufficient to authorize access to the private database” (see Examiner’s Answer at p. 20). The Examiner argues that “Garrison/Rezvani teach a more robust system, but at a minimum, some piece(s) of the data must be exchanged before a user will be granted access” (see *Id.*). In other words, the Examiner argues that since Garrison/Rezvani teach a more complex or robust electronic system, then Garrison/Rezvani must therefore teach the claim element of using only an appliance identification to authorize access to a private database. Appellants strongly disagree with these arguments because they are not supported in the actual teachings and suggestions in Garrison/Rezvani.

Garrison teaches a **complex** key exchange between a user and a server to identify a user and provide him or her with access to the server. Appellants respectfully ask the Board of Appeals to read paragraphs [0047 – 0049] and [0065 – 0068] in Garrison (these paragraphs teach a complex key exchange between the user and server). Further, Rezvani states that cellular phones have ESNs that uniquely identify the cellular phone. Rezvani, however, does not discuss ESNs in a context of using such a number to provide access to a private database. In other words, the combined teachings of Garrison and Rezvani never suggest that verification of “only” the ESN is sufficient to grant access to a database.

Third, the Examiner argues that Appellants are merely attacking Garrison and Rezvani individually and not analyzing the combined teachings. Appellants respectfully disagree. Appellants have discussed the teachings of Garrison and Rezvani individually and the teachings and suggestions of combining these references.

As noted above, Garrison teaches a complex key exchange between a user and server. Rezvani states that cellular devices have ESNs. There is no suggestion whatsoever to remove the complex key exchange in Garrison and replace this key exchange with the ESN in Rezvani such that “verification of only the appliance ID is sufficient to authorize access to the private database.” Appellants respectfully argue that the Examiner is

picking and choosing unrelated sentences or teachings from Garrison and Rezvani with hindsight of Appellants' invention to allegedly obviate the pending claims.

In view of the above, Appellants believe that all pending claims are in condition for allowance. Allowance of these claims is respectfully requested.

Respectfully submitted,

/Philip S. Lyren #40,709/

Philip S. Lyren
Reg. No. 40,709
Ph: 832-236-5529